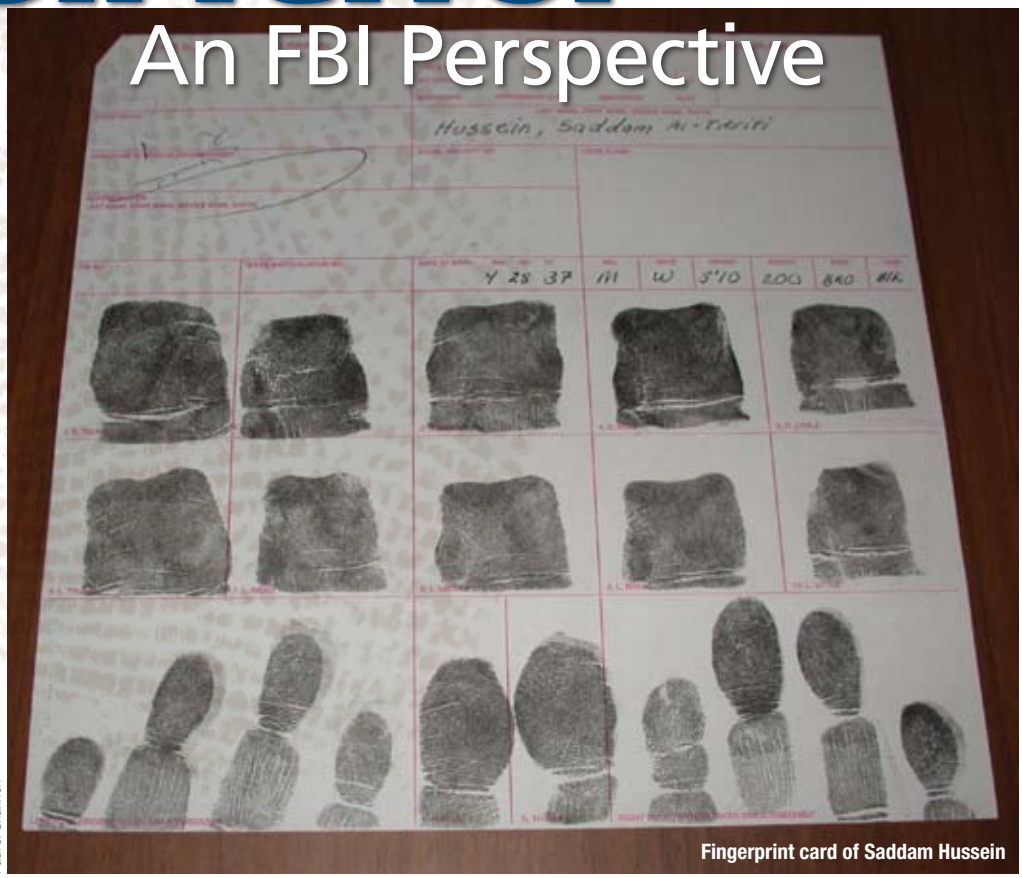
Fingerprints and the War on Terror

An FBI Perspective



Paul J. Shannon

Fingerprint card of Saddam Hussein

By PAUL J. SHANNON

In late 2001, with the Tora Bora bombing campaign in Afghanistan in full swing, a team from the Federal Bureau of Investigation (FBI) entered the combat theater on an unprecedented mission: to fingerprint, photograph, and interview captured terrorists as if they were bank robbers.

The idea of this mission was to freeze the identities of terrorists through a traditional law enforcement booking procedure used for decades by police officers in the United States to track dangerous criminals so the terrorists could always be identified as such.

There was urgency to this FBI mission. Afghanistan in 2001 was clearly the launching pad for the attacks of September 11. Under the rule of the Taliban, this war-torn country had become a haven for terrorists and enemies of the United States, even harboring Osama bin Laden's al Qaeda training camps. Islamic extremists had flocked to the camps by the thousands, over long-established clandestine routes from Europe, the Middle East, Asia, and Africa. Moreover, there was potential for the terrorists to use these same routes to scatter back to their home countries, where they would become undetectable as potential threats.

There was another factor creating urgency in this mission to freeze terrorists' identities: at the time of the invasion, the American military was not routinely fingerprinting detainees or sharing detainee information with U.S. law enforcement.

The urgency paid off quickly. A foreign fighter captured during the Tora Bora bombings claimed he was in Afghanistan to learn the ancient art of falconry. A fingerprint identification was made against his immigration record, showing that he was denied entry to the United States in August 2001 at Orlando International Airport by a suspicious immigration official. The individual was Mohamed al Kahtani, who would later be named by the

Supervisory Special Agent Paul J. Shannon, Federal Bureau of Investigation, is the Director for Law Enforcement Policy on the Homeland Security Council at the White House.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Fingerprints and the War on Terror: An FBI Perspective	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Institute for National Strategic Studies,260 5th Avenue SW Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**7**	

Paul J. Shannon

Author fingerprinting Saddam Hussein after capture

a foreign fighter captured during the Tora Bora bombings claimed he was in Afghanistan to learn the ancient art of falconry

9/11 Commission as the likely 20th hijacker. This person remained in U.S. custody.

Background

The Bureau's equipment on this first mission was primitive. Printer's ink, hand rollers, and paper cards were used to gather fingerprints. Descriptive data such as height, weight, eye color, hair color, date of birth, place of birth, and nationality were handwritten on these fingerprint cards. Detainees held erasable boards with their names and assigned numbers for mug shots, taken with a 35-mm camera. Oral swabs like oversized Q-tips were used to collect DNA samples. The gear fit in a briefcase that could be opened and used as a fingerprint platform.

As the Armed Forces transform to counter the threats of asymmetric warfare, we will soon be focusing on another new mission: the collection of biometric information from the foes we face on the battlefield.

The U.S. Government is building a comprehensive biometric screening regime to detect terrorists before they attack. Our border security, visa screening, and law enforcement systems are based primarily on fingerprints: permanent and unique identifiers that are difficult, if not impossible, to counterfeit or alter. So when a terrorist is captured in the field, or a safehouse is raided, it is important to "freeze" the terrorist's identity so that he can always be identified as an enemy and a potential threat. False names, passports, and nationalities cannot mask the data found in fingerprints or DNA.

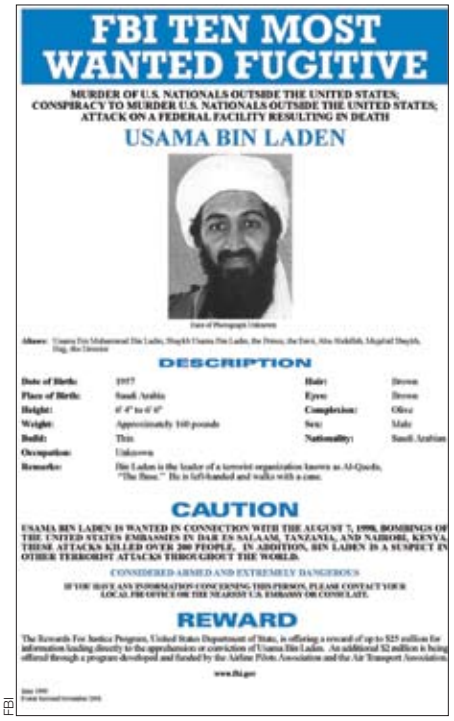
The Department of Defense, with the full support of the White House, has recognized the collection of biometric identification as a basic warfighting capability, especially when fighting insurgent enemies who hide among the civilian populations.

As Agent Paul Shannon states in this article, among the terrorists and insurgents that we are fighting overseas, roughly 1 in 100 has a criminal record in the United States, which means that many of the people we are fighting today not only have been in America and in our hometowns but also have committed a crime while they were here.

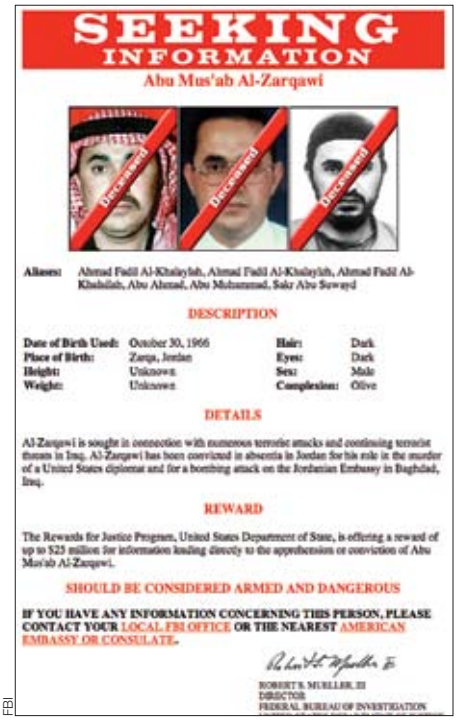
It is important that every biometric identifier—every fingerprint, photograph, DNA swab, or iris scan—is collected correctly and precisely the first time because there may be only this opportunity to ensure the safety of our troops, families, and nation.

We know this is a difficult mission, but we also know there is no one more capable than the men and women of the U.S. military to carry out this mission. America will continue to take the fight to those who wish us harm, and we will continue to protect both our citizens and interests. It will not be easy, but by using every tool at our disposal, we will win.

Frances Fragos Townsend is Assistant to the President for Homeland Security and Counterterrorism.



FBI Ten Most Wanted poster of Osama bin Laden



FBI Ten Most Wanted poster of Abu Mus'ab Al-Zarqawi

The team handed out these portable booking stations in Kandahar and Kabul. The agents fingerprinted detainees in U.S. custody there and in Northern Alliance custody in Mazar-e-Sharif. The FBI team, supported by U.S. troops and by deployed U.S. intelligence officers in theater, also worked for months along the Afghanistan-Pakistan border, fingerprinting foreign fighters who were captured trying to flee coalition forces.

The fighters were young, radicalized, and committed to jihad. A full quarter of them freely admitted to interviewers that they had surrendered in order to fight another day—a day of their choosing. They expected to be well treated, as al Qaeda trainers had explained U.S. policies toward prisoners. The message to the fighters was wait, and eventually you will be freed.

These self-declarations were by themselves reason to justify the FBI mission in Afghanistan and were of no surprise to the agents; the best predictor of future behavior is past behavior. A person who steals, lies, and commits acts of violence in his twenties is likely to do the same or worse later in life. Criminals also rarely give up when confronted by law enforcement. Instead, they try to remain anonymous and undetected. They lie about their identities to avoid punishment.

Once the booking packages were collected, terrorists' identities were permanently recorded. The FBI team then hand-carried the packages from Afghanistan to Clarksburg, West Virginia, where the Bureau acts as steward to the national criminal databases used by U.S. law enforcement nationwide. The two databases—the National Criminal Information Center (NCIC), a text-based system that officers can query with information such as name and date of birth, and the Integrated Automated Fingerprint Identification System (IAFIS), which positively identifies criminals by comparing submitted prints against known prints—can be called the backbone of U.S. law enforcement. On a typical day, NCIC is queried more than 3 million times and IAFIS compares over 70,000 submitted prints.

The team's idea was to post the terrorists' photographs and information in NCIC and place their fingerprints in IAFIS, with the result being ready identification when the terrorists attempt to enter the United States or American law enforcement encounters them. Authority was sought from the U.S. Attorney General to place the terrorists in these databases, which traditionally were comprised exclusively of domestic criminal information. The conventional databases could tell a user who had been arrested for robbing a bank in Dallas, committing a burglary in Newark, or forging a check in Seattle. They could not tell who learned to make an improvised explosive device in a terrorist training camp. This inability was what the FBI proposal to the Attorney General would change. A strong component of this proposal was the recognition that if a police officer had stopped one of the 19 hijackers from the September 11 attacks on the streets or in the airports, nothing in the databases would have alerted the officer to a threat.

In March 2002, the Attorney General approved the FBI proposal, not only endorsing the idea but also issuing a formal directive compelling the Bureau to gather terrorist fingerprints and descriptive data internationally and place this information in databases. Using this new authority, the FBI began adding fingerprints gathered in Afghanistan to IAFIS and almost immediately was confronted with a wholly unexpected finding. When the first batches of terrorist prints were added to IAFIS, identifications occurred at the rate of about 1 per 100 terrorists. That meant that not only had those terrorists been to our country, but they had also engaged in conduct that led to arrest. By exposing terrorists and networks that otherwise might not have been revealed, these identifications provided immediate security and intelligence gains for the country.

not only had those terrorists been to our country, but they had also engaged in conduct that led to arrest

An example shows the power of fingerprinting. A foreign fighter captured near the Afghanistan-Pakistan border claimed he was an itinerant preacher of Islam and not part of the fighting. He was one of many captured in the area with similar stories. The fingerprint identification was made against a misdemeanor marijuana arrest in an American city. When agents examined the arrest records, they determined that he was a flight student. This person remained in U.S. custody.

Such identifications were not aberrations. The Bureau team started what would become a worldwide effort to gather thousands of prints of known terrorists and search and post them through law

Detainee being released from Abu Ghraib Prison

U.S. Marine Corps (Ben Flores)

enforcement databases. In known terrorist populations sampled to date, and in Iraq today, the hit rate has remained close to 1 percent.

Hits have been recorded at a similar rate on pockets of detainees captured and then fingerprinted in the combat theater of Iraq, which was unexpected because under Saddam, Iraq was a country with closed borders. An interesting event occurred when an FBI team traveled to a remote desert camp on the Iraq/Iran border, the main base of the Mujahedin-e Khalq (MEK), a terrorist group dedicated to the overthrow of the Iranian government. The MEK members led a sparse, almost cult-like lifestyle where men could not have contact with women, material goods were renounced, and a group mentality held sway. Yet even in this austere environment, when the team fingerprinted about 3,800 MEK fighters, more than 40 hits were recorded against IAFIS.

To the agents on that original FBI team, and on the teams that deployed in 2003, 2004, and 2005 to detainee camps in Baghdad, Mosel, Erbil, and Basra, the consistent rate of identifications against the domestic criminal fingerprint database provided stark conclusions about the nature of the enemy and the battlefield. As the team leader for forensic collection in Afghanistan and Iraq, and the agent who negotiated the terrorist fingerprint exchanges with certain allied countries, I would phrase the conclusions as follows:

- Terrorists are internationally mobile, criminally sophisticated, adept at crossing borders undetected, and adroit at obtaining multiple forms of false identifications.
- Anonymity is the greatest weapon, and the challenge for a Soldier or police officer is to pick the terrorist out of the crowd.
- Terrorism is closely associated with criminality. In fact, under the U.S. system, terrorists who make it to America must be prosecuted in a court of law. Terrorist databases cannot be maintained separately from criminal databases.
- Fingerprints, correctly collected in law enforcement fashion and placed in databases, are the best way to track and identify terrorists. Name and birthdate databases are of limited value against an enemy who hides his identity.
- The battlefield is global. Terrorists bide their time and wait out the immediate conflict to attack later.

Federal Framework

It is critical to homeland security that the military develop what have traditionally been considered law enforcement equities, identify terrorists and enemies of the United States, and share the gathered fingerprints, photographs, DNA, descriptive data, and trace evidence, such as latent fingerprints (fingerprints not readily visible to the naked eye), with U.S. law enforcement. Five years of work by FBI teams gathering terrorist prints led to this conclusion. At the White House, working through the Homeland Security Council and the National Security Council, this conclusion has been the foundation of a policy statement on the role of the American military in the forensic identification of terrorists. According to the statement, comprehensive biometric screening for terrorists, especially using fingerprints, will be basic to homeland security, protection of U.S. troops in combat zones, and identifying previously unknown terrorists. The Department of Defense (DOD) will help in this effort in two major ways: taking full sets of 10 fingerprints for all detainees from overseas operations, and collecting and keeping latent fingerprints and additional forensic identification from the sites of terrorist activities.

At the Homeland Security Council, policy work is in large part directed by Presidential directives. The underlying directive for this policy statement about the U.S. military is Homeland Security Presidential Directive (HSPD) 11, signed and issued in August 2004. This directive calls for improving terrorist screenings of people, cargo, and conveyances at opportunities outside, at, and within national borders. The military's role in the effort has been substantial, but the considerable advances in the overall enterprise are due to it being interagency and Government-wide. Screening relies not only on those agencies conducting the screenings but also on those serving as collectors, who add to the database as they encounter terrorists abroad and wherever combat takes place. This procedure dovetails with the screening process for visitors to the United States, where names are compared with the date-of-birth watch lists being compiled for the National Center for Counter Terrorism's Terrorist Screening Database.

Until recently, the Federal Government had three major agencies—the Departments of Homeland Security (DHS), Justice, and Defense—that were building terrorist screening databases and biometric systems that could not efficiently share information. DHS and DOD had 2-print screening systems that could not interface with Justice or with the FBI national criminal database, which was based on the traditional law enforcement standard of 10 fingerprints. Through HSPD 11, these agencies have adopted the 10-print standard and are building systems that will be interoperable, connecting law enforcement, border security, and military detainee systems to detect terrorists better before they attack.

the overarching directive is to improve terrorist screening through consolidation of screening activities throughout government

Vehicle destroyed by car bomb

Paul J. Shannon

Latent fingerprints discovered on car bomb vehicle

Paul J. Shannon

Significant force protection gains in Iraq and other theaters have already been realized, and identifications have been made against IAFIS of prints gathered by the military.

The overarching directive from HSPD 11 is to improve terrorist screening through consolidation and coordination of disparate screening activities throughout government, and the Homeland Security Council has sought to assist through the interagency process, promoting information-sharing, and Federal standards. Examples of progress include:

- the adoption of a 10-print standard for the biometric screening of all foreign visitors to the United States, including applicants for visas at U.S. Embassies worldwide
- DOD adoption of the 10-print standard in processing military detainees, in particular for insurgent and foreign fighters encountered in combat theaters, and the immediate sharing of this information with U.S. law enforcement
- the Department of State series of overt diplomatic contacts with allies in the war on terror to negotiate agreements to share terrorist screening information, including forensic identifiers such as fingerprints
- Homeland Security Council meetings with law enforcement and intelligence agencies with the goal of fully involving them in collecting terrorist fingerprints and latent prints internationally.

Through HSPD 11, the Homeland Security Council seeks to begin robust international collection of terrorist screening information such as fingerprints. This process must be systematic, sustained, and worldwide, as our screening systems will be only as good as the database against which suspects are checked. This process must also be a managed effort by multiple agencies, as collection is most effective at first point of contact with known or unknown terrorists. The Department of Defense (in combat theaters primarily), Central Intelligence Agency, and National Security Agency are most often the first responders overseas who will have that initial contact.

Other countries, some allies in the war on terror and some not, have significant existing databases of terrorists that would greatly enhance our own. Some countries are safe havens and could provide access to terrorist populations. Collection of screening information can occur through four channels: *overt*, through diplomatic agreements which would be managed by the State Department and would likely be a long-term process; *informal*, through established law enforcement channels, which would be managed by the Bureau; *covert*, when a host country is uncooperative or hostile, which would be managed by the Intelligence Community; and *direct*, through encounter with terrorists and their implements in combat theaters, which would be managed by the military.

Soldiers Meet Agents

In early 2005, the U.S. military committed to adopting a booking procedure for detainees in Iraq and other theaters that meets law enforcement standards with respect to fingerprints, photographs, and mandatory descriptive data. By memorandum and general order, it was mandated that all DOD detainees be processed to U.S. law enforcement standards. Detainees are specifically to be fingerprinted with 10 rolled and 10 flat prints, which are then shared with law enforcement because of the transnational nature and mobility of the terrorist fighter. Fingerprint-based background checks, also on the 10-print standard, were similarly ordered for foreign nationals applying to work on U.S. military bases and in some Iraqi agencies, such as military and police forces.

These commitments have led to immediate short-term benefits for the military in the Iraqi theater, such as better control of detainee populations, improved force protection for American bases in theater, and identifications against fingerprint databases, which allow military intelligence officers to focus interrogations on the worst terrorists.

As laudable as the gains have been, the U.S. military's status quo on forensic identification in theater, and specifically on fingerprints, remains half a program.

The terrorist crime scenes in such theaters as Iraq, Afghanistan, Colombia, and the Philippines are not being fully exploited for forensic identification in the way U.S. law enforcement would process a murder, rape, or robbery crime scene for trace evidence that would then be preserved to identify the offender. Thus, there are missed opportunities in the short term to wage battle better by identifying and neutralizing insurgents on the ground in theater, and missed opportunities in the long term to secure the homeland, as

latent prints can be placed permanently in law enforcement and border security fingerprint databases for future identifications.

Forensic identifiers, such as latent fingerprints, have no shelf life limit. They are permanent identifiers made against correctly gathered latent prints 40 and 50 years after a crime. Latent prints can also be placed in automated systems such as IAFIS for identifications of unknown terrorists who might try to enter the country during or after the war in Iraq, be it 5, 10, or 50 years from today. Latent prints gathered in Iraq would thus have lasting value to homeland security and contribute significantly to the war on terror.

Recommendations

To institute a full forensic identification program in theater and within DOD, the military must:

- deploy crime scene teams within the combat theater to use simple, well-established techniques to collect and preserve evidence
- establish procedures based on best practices of U.S. law enforcement to track the collection of evidence for later use in U.S., Iraqi, or international courts
- formalize a manner for transferring evidence collected in theater to the U.S. law enforcement laboratories for full exploitation.

Crime Scene Teams. Events recently unfolding in some locations demonstrate that there is urgency for implementing these proposals. Sites discovered in Fallujah included the apparent scene where hostages held by the Abu Musab al-Zarqawi organization were beheaded, as well as an apparent headquarters of al-Zarqawi, including letters written by him. Neither location appears to have been forensically exploited. Other significant, high-value sites not forensically exploited are the hiding hole where Saddam was captured and the shed from which he directed insurgent activity. Minimal effort, supplies, and training could have yielded significant trace evidence from such sites, such as latent fingerprints, hair, fiber, and DNA that could lead to positive, court-accepted identification of victims, perpetrators, and conspirators.

high-value sites not forensically exploited are the hiding hole where Saddam was captured and the shed from which he directed insurgent activity

Latent prints in particular would have immediate value to the U.S. military in Iraq. Searches of these prints against automated databases can take a relatively short period of time but can identify previously unknown terrorists. Hits made against the in-theater database could lead to operations to neutralize terrorists. Moreover, hits reflecting that the terrorists had been in the United States would lead to investigations in the homeland.

The long-term value of latent prints, if searches do not yield immediate hits, is considerable:

- Unidentified latent prints can be placed in U.S. fingerprint databases for future identifications.
- Latent prints are retained for comparison against detainees or fighters in other theaters, such as Afghanistan and the Philippines.
- Latent prints can be shared with allies the same way as intelligence for search against their automated systems and postings for future identifications.
- Latent prints, once identifications are made, are admissible as evidence in U.S., Iraqi, and international courts.
- As part of the rebuilding effort in Iraq, Iraqi security forces are being taught to fingerprint criminals and insurgents, and a commitment has been made that the United States will build an automated fingerprint system for these forces.

Evidence Collection. The cost of gathering latent prints is minimal. There is no expensive logistic apparatus to establish, but simply a formalization of the existing pathway to transfer evidence collected from the field to the laboratory and the creation of as complete an evidence chain (that is, documentary support of where and by whom evidence was gathered) as the ebb and flow of combat allows. The key to success is seizing all opportunities, and then gathering evidence properly. Facilitating the search in the short term would require designating three-man mobile teams that would deploy to high-value sites and operations in theater, much as crime scene teams in major cities respond to crime scenes discovered by patrol officers and then process those scenes. The FBI's basic instruction for evidence collection can be given in a 40-hour week. A more advanced course requires 2 weeks. While certain lab techniques for developing and comparing latent prints and other trace evidence are complex and require considerable training and expertise, collecting trace evidence is basically simple. One team member photographs and documents evidence while the other two collect and preserve, a process known as "bagging and tagging."

This procedure also lends itself to the need in the combat theater to get off the exploited site quickly. If the team knows what constitutes good evidence, it can collect and preserve a great deal in a short time.

Such a process, including photographing and documenting, could be accomplished in minutes with equipment that could fit in a backpack. The gains include a permanent record of the terrorist act and forensic identifiers to discover the perpetrator and prosecute the act as a terrorist crime.

The law enforcement commitment in the short term, primarily from the FBI, would be to train these teams, provide expert advice on the types and amounts of equipment necessary, and provide samples of standard administrative procedures and the documents used to track evidence for purposes of proving criminal acts in a court of law. Based on basic equipment for FBI Evidence Response Teams, a 3-man team could be outfitted for several weeks for about $2,500. The Bureau would also have to commit to taking in larger volumes of evidence from Iraq, which at present amounts to only a fraction of work received by the FBI laboratory.

Evidence Transfer. The framework for getting evidence from field to laboratory already exists in a process that balances immediate in-theater requirements with the need to develop trace evidence in a laboratory setting. In September 2003, the military with the FBI set up the Combined Explosive Exploitation Cell to analyze improvised explosive devices that coalition forces collected in Iraq. The mandate for the cell was to conduct a quick forensic triage of devices and report back to the theater regarding design, appearance, triggering mechanism, and anything else that could help a Soldier in the field recognize, avoid, or neutralize an explosive apparatus. In this process,

Taking digital identification photo of detainee

1st Combat Camera Squadron (Suzanne M. Day)

Paul J. Shannon

Comparing latent print to print in database

1st Combat Camera Squadron (Suzanne M. Day)

Fingerprinting detainee in Tikrit

while creating a product that definitely saved lives, it was recognized that the devices should also be exploited in a law enforcement manner for trace evidence—DNA, hair, unique tool marks, explosive analysis, or latent prints.

In October 2003, the cell began forwarding devices to the FBI laboratory through the Bureau's command post in Baghdad. More than 800 devices have since been sent to the laboratory, processed through the new Terrorist Explosive Device Analytical Center. Technicians process the items for latent prints and other trace evidence. The prints are then searched and posted permanently in IAFIS for future identifications. Analysts also produce reports on devices that are distributed to U.S. law enforcement bomb squads and explosive technicians nationwide, to disseminate domestically the same intelligence on explosive devices that has been passed back to soldiers in the combat theater.

the mandate for the cell was to report anything that could help a soldier in the field recognize, avoid, or neutralize an explosive apparatus

Several devices have been linked through latent comparison showing that the same bomb maker worked on them, while others have been linked through DNA comparison.

Crime scene work and evidence collection must become part of the institutional goals of the military and an integrated part of combat operations. Crime scene teams must be present at high-value sites in the aftermath of suicide car bombings and attacks, and on the battlefield during campaigns such as the taking of Fallujah. Soldiers must behave as first responders—in the same manner as U.S. police officers, firefighters, and paramedics—in recognizing a high-value scene, understanding that evidence there must be preserved, and knowing they must call in crime scene teams. The evidence collected must then be exploited and passed back to U.S. law enforcement and border security because of the international mobility of the terrorist fighter.

According Department of State statistics, 87 percent of terrorist attacks against Americans or their interests worldwide have involved improvised explosive devices. This trend will continue as Iraqi-trained terrorists bleed out of Iraq into surrounding countries and Europe and as al Qaeda's preference for large car bombs that inflict maximum casualties shows no abatement. The terrorist's and the insurgent fighter's greatest weapon is anonymity, and the most difficult task for a Soldier or a law enforcement officer in the war on terror is to pick that individual out of the crowd. Forensic identifiers such as latent prints and DNA give the United States the potential to identify the most dangerous subset of terrorists, unknown bombmakers. **JFQ**